1. **ESPECIFICACION TECNICA:** Desarrollo del Sistema de Información para Atención de Emergencias SECAD.

2. **UNIDAD SOLICITANTE:** Oficina de Tecnologías de la Información y las Comunicaciones OFTIC - Grupo de Desarrollo de Software GUSOF.

3. **VIGENCIA**: La presente especificación tendrá una vigencia de un año (01), pero estará sujeta a ser actualizada permanentemente de acuerdo a la vigilancia tecnológica que se establezca sobre el elemento a adquirir, con el objeto de que esta responda en todo momento a las necesidades y exigencias de la Policía Nacional.

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
1	**GENERALIDADES**		
1.1	El contratista deberá realizar el desarrollo a la medida de acuerdo a las necesidades de la Policía Nacional, utilizando lenguajes y tecnologías de código abierto sin dependencias propietarias para funciones críticas. Lenguajes principales: TypeScript, Java o Python o C# .NetCore (últimas versiones estables). La arquitectura utilizada deberá estar enfocada en Microservicios contenerizados (Docker/Kubernetes): Servicios globales: Auth, Tenant Resolver, Connection Pool Manager, API Gateway, Analytics ETL. Servicios por tenant: CAD Core, Dispatch Engine, GIS, Communication Hub, AI Service. Servicios edge: microservicios mínimos de despacho en nodos locales.		
1.2	Todos los desarrollos, integraciones, funcionalidades y demás implementaciones diseñadas específicamente para este proceso, serán propiedad exclusiva de la Policía Nacional. Queda estrictamente prohibida su reproducción, réplica o utilización para fines distintos a los establecidos en este contrato, salvo autorización previa y por escrito de la Policía Nacional.		
1.3	Todo el sistema deberá estar integrado con el LDAP de la Policía Nacional (OUD de Oracle) como proveedor de identidad principal, con mecanismo de fallback a base de datos local de usuarios cifrada cuando OUD no esté disponible.		
1.4	El contratista deberá realizar levantamiento de información necesaria que permitirá dar cumplimiento a cada uno de los requerimientos mínimos establecidos en el presente proceso, utilizando los formatos definidos por la Policía Nacional. Deberá realizar mesas de trabajo técnico-operativas para levantamiento de historias de usuario, definición de campos de formularios, catálogos de tipificación, preguntas orientadoras y parametrización general de los módulos.		
1.5	El contratista deberá hacer uso de librerías y plugins con comunidad activa o soporte del fabricante. El sistema debe contar con una interfaz web accesible desde navegadores estándar: Microsoft Edge, Mozilla Firefox, Google Chrome y Safari. El contratista deberá especificar las versiones compatibles de cada navegador.		
1.6	El contratista deberá realizar todas las pruebas necesarias acordadas al inicio del proyecto para garantizar la aprobación técnica y funcional del sistema: (1) Pruebas unitarias: verificar que cada componente funcione correctamente de manera aislada. (2) Pruebas de integración: comprobar la interacción entre módulos. (3) Pruebas funcionales: validar que el sistema cumpla con los requerimientos. (4) Pruebas de usuario: asegurar que el sistema cumple con las expectativas de usuarios finales. (5) Pruebas de rendimiento: evaluar velocidad, estabilidad y escalabilidad. (6) Pruebas de seguridad: garantizar protección de datos y cumplimiento normativo. El contratista entregará una **suite de pruebas automatizadas** (unitarias y de integración) ejecutable en el pipeline de entrega, con resultados visibles por commit.		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
1.7	El contratista deberá implementar el sistema de información desarrollado en servidores de pruebas, con el propósito de realizar las siguientes evaluaciones: • Pruebas de estrés. • Pruebas de rendimiento. • Pruebas de conectividad. • Evaluaciones de tiempos de respuesta. • Verificación del cumplimiento de los requerimientos del software. Estas pruebas permitirán analizar el comportamiento del sistema y la arquitectura implementada. El periodo de pruebas deberá tener una duración no inferior a 30 días posteriores a su publicación, y los resultados deberán ser validados por la Oficina de Tecnologías de la Información y las Comunicaciones - OFTIC y el usuario líder funcional. Durante este periodo, cualquier inconsistencia o irregularidad identificada que incumpla con las capacidades esenciales, requerimientos funcionales o no funcionales deberá ser subsanada. En caso de requerirse un ajuste adicional, este podrá realizarse en un plazo no superior a 90 días, garantizando la resolución de los problemas antes de la entrega final y la aceptación a satisfacción. El contratista entregará un **banco de pruebas de carga reproducible con múltiples CAD simultáneos**, con el perfil de carga y los umbrales de aceptación [a definir en mesas de trabajo], y los resultados se anexarán al acta de pruebas.		
1.8	Se deberá garantizar la validación del sistema en el entorno de producción mediante pruebas de pilotaje, señaladas en el ítem 1.6. Los escenarios de prueba serán seleccionados por el usuario funcional y el periodo de pilotaje deberá tener una duración no menor a 60 días ni mayor a 90 días. Este proceso deberá completarse antes de la entrega final y la aceptación a satisfacción, asegurando el correcto funcionamiento del sistema en condiciones reales de operación.		
1.9	Se deberán utilizar componentes en una de sus últimas versiones estables disponible en el mercado, debidamente liberados por el fabricante y acompañados de su matriz de compatibilidad (librerías, plugins, frameworks). Dichos componentes no deberán generar costos adicionales para la Policía Nacional y deberán ser de código abierto (Open Source).		
1.10	El contratista será responsable de la instalación de los ambientes correspondientes (Desarrollo, Pruebas y Producción) para el software entregado, asegurando su correcta configuración y puesta en marcha en cada uno de ellos.		
1.11	El contratista deberá elaborar un cronograma de trabajo detallado para el proyecto a desarrollar, en el cual se describan las actividades previstas y los plazos de cumplimiento. El cronograma debe incluir, entre otros documentos, el acta de inicio del proyecto y los puntos clave para su seguimiento.		
1.12	Se deberá garantizar el cumplimiento de las buenas prácticas de desarrollo seguro definidas por el contratista al inicio del proyecto. La Oficina de Tecnologías de la Información y de las Comunicaciones, realizará pruebas de vulnerabilidades sobre los desarrollos entregados por el contratista. Cualquier vulnerabilidad identificada deberá ser subsanada en su totalidad por el contratista en un plazo no superior a 50 días, sin perjuicio de que las pruebas sean evaluadas nuevamente una vez realizados los ajustes.		
1.13	El contratista deberá presentar, dentro de los primeros quince (15) días calendario contados a partir de la fecha del acta de iniciación del contrato, un plan detallado del proyecto. Este plan debe incluir un cronograma de trabajo que contemple las siguientes fases: levantamiento de información, análisis, diseño, construcción, pruebas, aceptación, implementación y capacitación, así como los eventos y productos finales asociados a cada una de ellas. Adicionalmente, el contratista deberá entregar un detalle de la arquitectura propuesta (a alto nivel), junto con el plan de trabajo necesario para todas las integraciones solicitadas. Este plan deberá ser aprobado por la supervisión del contrato antes de su ejecución.		
1.14	El contratista deberá entregar la siguiente documentación en idioma castellano, asegurando que cumpla con los estándares requeridos para la implementación y operación de la solución:		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
	1. Manual de usuario final: Instrucciones detalladas para que los usuarios puedan operar la solución de manera efectiva, incluyendo ejemplos prácticos y resolución de problemas comunes. 2. Manual técnico de la solución implementada: Documentación técnica que describa la arquitectura, configuraciones, dependencias y cualquier otro aspecto necesario para el mantenimiento y actualización de la solución. 3. Modelos de arquitectura: Representación gráfica y descriptiva de la arquitectura de la solución, incluyendo los componentes, interacciones y flujos principales del sistema. 4. Modelos de casos de uso: Diagramas y descripciones que detallen los diferentes escenarios de interacción entre los usuarios y el sistema, especificando las funcionalidades principales y secundarias. 5. Modelos entidad / relacional: Diagramas que representen la estructura de la base de datos, detallando las entidades, relaciones y atributos utilizados en la solución.		
1.15	El contratista deberá realizar el despliegue del compilado del proyecto en el entorno administrado por la Policía Nacional, cumpliendo con las políticas de seguridad institucionales. La entrega final del proyecto deberá hacerse en el repositorio de DevOps administrado por OFTIC, con: rama master actualizada, historial completo de cambios, estructura estándar de proyecto y validación final por el equipo técnico de OFTIC.		
2	**CAPACIDADES ESENCIALES**	**CUMPLE**	**NO CUMPLE**
2.1	Las capacidades esenciales descritas en este numeral corresponden al alcance mínimo operativo que el contratista deberá entregar al concluir el mes 6 del proyecto.		
2.2	**Gestión Integral de Comunicaciones:** recepción y procesamiento de reportes por voz (línea 123 integrada con planta telefónica institucional), chat, SMS, fotografías y video. Capacidades de transcripción de voz a texto habilitables o deshabilitables por el administrador sin afectar la operación general.		
2.3	**Asistencia Automatizada e Inteligencia Operacional:** reducción de la carga cognitiva del operador mediante verificación automática de ubicaciones, prevención de duplicidades, priorización por gravedad y recomendación de recursos cercanos al tiempo real.		
2.4	**Visualización y Coordinación Geoespacial (GIS):** módulo GIS avanzado 2D como núcleo de coordinación, con imagen operativa común, geocercas, rutas dinámicas y acceso a cámaras georreferenciadas a través del VMS institucional.		
2.5	**Seguridad e Interoperabilidad:** encriptación en tránsito y en reposo, controles de acceso estrictos y auditoria de uso.		
2.6	**Administración Nacional de CADs:** gestión centralizada del ciclo de vida de todos los tenants (CADs) desde la aplicación, con monitoreo de salud, onboarding, configuración y control de conectividad por territorio		
3	**ARQUITECTURA MULTITENANT FEDERADA**	**CUMPLE**	**NO CUMPLE**
3.1	El sistema de información debe implementarse bajo el modelo DB-per-Tenant: aplicación única centralizada en Bogotá, con base de datos operativa aislada por CAD. Cada CAD territorial mantiene soberanía total sobre sus datos y puede operar de forma autónoma ante pérdida de conectividad.		
3.2	**Esquema Master — Bogotá**: El esquema master alberga exclusivamente los componentes de enrutamiento y autenticación global. No contiene datos operativos de ningún CAD.		
3.3	**Flujo de autenticación OUD y 2FA con fallback:** El sistema implementa autenticación dual para garantizar continuidad operativa ante indisponibilidad del directorio institucional. 1. Pantalla de login Usuario ingresa login + contraseña. Sin necesidad de ingresar código DANE. 2. API Gateway → OUD → 2FA: Sistema autentica contra OUD institucional (LDAP/S). Si OUD responde: flujo normal. 3. OUD → Tenant Resolver: OUD valida credenciales, el servicio 2FA valida código TOTP y otro servicio centralizado retorna atributos del usuario, incluyendo código DANE o unidad organizacional.		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
	4. Tenant Resolver → tenants: Sistema consulta tabla tenants por código DANE y obtiene id_tenant. 5. Connection Pool Manager Obtiene y descifra credenciales de BD vía Vault. Emite JWT con id_tenant, roles locales y TTL. 6. OUD no disponible: Si OUD presenta timeout o error, el sistema autentica contra la tabla local_users_fallback (credenciales cifradas localmente). El operador accede con funcionalidad completa. El evento se registra con flag 'modo_fallback=true'. La Policía Nacional es responsable de la disponibilidad, mantenimiento y correcta gestión de los usuarios en OUD. 7. El sistema tendrá la posibilidad de validar usuarios y credenciales de personal civil o de otras entidades públicas. Las credenciales de las bases de datos de tenant NUNCA viajan al cliente ni se incluyen en el JWT. El desencriptado ocurre exclusivamente en el backend mediante Vault. Rotación automática de credenciales cada 90 días.		
4	**RESILIENCIA — TRES NIVELES DE OPERACIÓN**	**CUMPLE**	**NO CUMPLE**
4.1	1. **Normal:** Conectado a Bogotá. Todas las escrituras van a BD primaria central. Réplica local sincronizada en standby. 2. **Degradado:** Latencia WAN supera umbral configurable. Conmutación silenciosa a réplica local write-capable. Alerta automática al monitoreo central. 3. **Offline:** Pérdida total de conectividad (aplica especialmente para Vaupés, Amazonas, Vichada, Guainía, zonas PDET (Programas de Desarrollo con Enfoque Territorial.)). El servidor edge local opera como primaria. Funcionalidad completa equivalente al SECAD actual. Reconciliación automática al restaurar enlace (máx. 15 min). 4. Criterios de aceptación: conmutación entre niveles sin pérdida de casos en curso; operación autónoma de un CAD sin enlace con funcionalidad equivalente a la normal; reconciliación automática al restablecerse el enlace en el tiempo definido, con **resolución de conflictos documentada y auditada**. Se demostrará con **pruebas de desconexión controladas** [protocolo a definir].		
5	**ANALÍTICA NACIONAL CONSOLIDADA**	**CUMPLE**	**NO CUMPLE**
5.1	Un proceso ETL/ELT (Apache Airflow) extrae datos anónimos y agregados de cada BD de tenant hacia un Data Warehouse centralizado en Bogotá. Los datos sensibles se pseudoanonimizan antes de pasar al DW, cumpliendo la Ley 1581 de 2012. Las consultas de BI y reportes nacionales apuntan exclusivamente al DW, sin afectar el rendimiento operativo de los CADs.		
6	**REQUISITOS MÍNIMOS OPERATIVOS - REQUISITOS FUNCIONALES**		
6.1	Durante los meses seis a doce, el contratista deberá entregar los requisitos funcionales descritos en este numeral, que completan el alcance total de la plataforma, integrándolos con las capacidades esenciales descritas en el numeral 2 entregados al concluir el mes 6. Al finalizar este período, la totalidad de los módulos descritos en los Requisitos Funcionales deberá estar en operación productiva.		
6.2	**Integración con Agencias:** El sistema dispondrá de un único endpoint REST para salida (envío de casos a agencias) y un único endpoint REST para entrada (recepción desde agencias), bajo estándar EDXL-DE (Lenguaje de Intercambio de Datos de Emergencia - Elemento de Distribución) o similar. La plataforma deberá permitir la conexión simultánea de N agencias externas, mediante un único punto de entrada (endpoint de ingreso) y un único punto de salida (endpoint de egreso) por dirección de flujo. La habilitación de cada agencia estará condicionada a su existencia operativa y al cumplimiento del protocolo de integración definido. La lógica de transformación de protocolos específicos de los sistemas receptores es responsabilidad de cada agencia. El contratista entregará documentación técnica (Swagger o		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
	similar). Responsabilidad Policía Nacional: habilitar APIs de los sistemas institucionales (GESPO, VMS, ARCGIS) y proveer credenciales de acceso. Se deberá contar con el módulo que permita registrar agencias, debe contar miniimo con la siguiente información (información de contacto, jurisdicción, cobertura, especialidades, capacidad y horarios. Historial de cambios con trazabilidad completa). Por cada agencia saliente, el sistema permitirá configurar el modo de autenticación (sin autenticación, token, autenticación básica o clave de API), cabeceras adicionales, formato del mensaje (plano o estructurado) y mapeo de campos. Incluirá vista previa del mensaje que se enviaría y recepción de actualizaciones de estado enviadas por la agencia. Toda comunicación entrante o saliente quedará auditada con el mensaje y la respuesta completos. Cada CAD o Tenant tendrá sus propias llaves de API para las integraciones entrantes. Cada llave pertenecerá a un solo CAD y tendrá alcance por canal. El sistema permitirá emitirla, regenerarla, activarla, desactivarla y probarla, y entregará una ficha técnica por canal. El revelado de una llave quedará auditado con usuario, IP y fecha. El canal de despacho de un caso entrante lo fijará la plataforma, no el sistema externo que lo envía.		
6.3	**Usuarios / Roles / Perfiles:** RBAC con mínimo privilegio, herencia de permisos, MFA, gestión de sesión (caducidad, bloqueo, cierre remoto). Integración con OUD institucional como primario. Mecanismo de contingencia (fallback): base de datos local de usuarios cifrada cuando OUD no esté disponible. La disponibilidad, mantenimiento y gestión de usuarios en OUD es responsabilidad exclusiva de la Policía Nacional. Integración con método de doble autenticación institucional 2FA. Los roles podrán tener fecha de vigencia y justificación obligatoria. El menú de la aplicación será administrable por rol. Cada CAD declarará cuáles roles son administrativos, y los permisos se asignarán por casillas.		
6.4	**Administración local de usuarios:** Permite la creación de usuarios (miembros de la institución y miembros de otras entidades) y roles en cada CAD. El sistema permitirá administrar entidades, sus canales de atención y la asignación de cada usuario a entidad, canal de despacho y cola telefónica. El sistema permitirá administrar la línea de mando (grado, cargo y jerarquía) y catálogos de dominio jerárquicos con vigencia.		
6.5	**Administración Nacional de CADs**: Módulo integrado en la plataforma para la gestión del ciclo de vida de todos los CADs (tenants) a nivel nacional, accesible exclusivamente por administradores de plataforma. Permite: registro de nuevos CADs, gestión de credenciales de BD, asignación de categoría de conectividad, monitoreo de salud en tiempo real, activación/desactivación de tenants, configuración de feature flags y mapeo de atributos OUD. Centralizada de todos los CADs (tenants) del país, accesible desde la aplicación exclusivamente por administradores de plataforma con rol. Permite gestionar el ciclo de vida completo de cada CAD sin intervención sobre el código fuente ni la base de datos directamente. Funcionalidades: (1) Registro de nuevos CADs con código DANE, nombre, departamento, municipio y categoría de conectividad (A/B/C); (2) Configuración segura de		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
	credenciales de base de datos del tenant (cifrado automático vía Vault, sin exposición en pantalla); (3) Activación, desactivación y suspensión de CADs; (4) Asignación y modificación de categoría de conectividad; (5) Configuración de atributos OUD por tenant (mapeo código DANE ↔ id_tenant); (6) Gestión de feature flags por CAD (habilitar/deshabilitar módulos o funcionalidades específicas); (7) Configuración de parámetros operativos por territorio (jurisdicciones, agencias disponibles, protocolos); (8) Dashboard nacional en tiempo real con estado de salud de cada CAD (Nivel 1/2/3 de conectividad); (9) Indicadores de uso y rendimiento por tenant; (10) Flujo de onboarding guiado paso a paso para incorporar nuevos CADs; (11) Registro auditable de todas las acciones administrativas sobre tenants. Catálogo nacional de unidades policiales, con carga e intercambio mediante hoja de cálculo. Catálogo de sitios de grabación (unidad que opera dentro de un CAD). Varias unidades podrán compartir un CAD sin mezclar sus registros, y el mapa abrirá donde trabaja cada una. Los superadministradores se registrarán en la base maestra y se administrarán desde la aplicación. El último activo no podrá retirarse. Al cambiar de contexto entre CAD se revalidará la sesión, con aviso visible de «administrando otro CAD». El superadministrador gestionará los códigos de caso a nivel nacional. Se configurarán los umbrales del monitor de salud (intervalo, tiempo de espera, latencia degradada y fallos consecutivos) y se conservará el historial de salud.		
6.6	**Gestión de Migraciones de Schema BD:** Interfaz para visualizar el estado de las migraciones de base de datos (Flyway/Liquibase Licenciamiento Open Source) en todos los tenants: versión de schema actual por CAD, historial de migraciones aplicadas, identificación de tenants desactualizados y disparo controlado de actualizaciones de schema. Solo accesible para administradores con rol DBA nacional.		
6.7	**Turnos de vigilancia y Posición de Recursos en Campo:** Captura y procesamiento en tiempo real de la ubicación de recursos en terreno. La información se obtiene de la integración con el sistema GESPO institucional. La Policía Nacional habilitará las APIs de GESPO y proveerá permisos y credenciales para la integración. Creación de turnos de vigilancia asociados a una agencia, para el caso de Policía Nacional el turno y los recursos asociados serán consultados en GESPO mediante APIs y guardados en el SECAD. Para el caso de otras agencias, los turnos deberán crearse de forma manual, así como los recursos asociados, esto aplica también para Policía Nacional. Copiar un turno a otra franja, importar unidades desde el sistema institucional de minuta de vigilancia y sincronizar la posición de las unidades con el sistema de ubicación institucional. Cada recurso registrará su origen (manual o automático), personal asignado, canal de radio y bitácora de cambios de estado, con resumen de disponibilidad en vivo. Las franjas horarias del turno servirán de filtro en reportes, mapas y casos.		
6.8	**Recepción de Llamadas:** Centraliza las comunicaciones de emergencia recibidas por distintos canales. Registro estructurado mediante formularios predefinidos y configurables. ID único e irrepetible por incidente (con prefijo código DANE para unicidad nacional). Detección automática de duplicidades. Ciclo de vida completo. Ficha de evento con campos mínimos: ID, tipo, ícono de estado, localización geográfica, descripción, propietario, creador, fechas y documentos anexos. Clasificación diferencial por población vulnerable. Los campos del formulario serán definidos por la Policía Nacional en las mesas de trabajo iniciales.		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
	Registro y gestión de casos por: (1) Voz - Línea 123 integración con la planta telefónica que permita extraer datos de la llamada, como el número de abonado u otros datos relevantes que se pueda obtener; (2) Chat - el sistema deberá disponer de un endpoint API REST para la recepción de conversaciones de chat, a partir de las cuales se creará automáticamente un incidente en la plataforma con la información extraída de la conversación; (3) SMS - el sistema deberá disponer de un endpoint API REST para la recepción de mensajes de texto, generando automáticamente un incidente a partir del contenido recibido; (4) Fotografías - el sistema deberá dispondrá de un endpoint tipo API REST para la recepción de imágenes, las cuales serán adjuntas al incidente previamente creado por canal de chat o mensaje de texto; (5) Video en vivo - enlace único y temporal enviado a dispositivos PDA de unidades en campo, activado por interacción del usuario (WebRTC), sujeto a compatibilidad del navegador del dispositivo. La Policía Nacional es responsable de la compatibilidad de hardware y conectividad de los dispositivos PDA a través de una (1) integración API REST. Integración con servidores de Abonado Llamante (Operadores de telefonía) para obtener coordenadas verificadas y actualizadas en tiempo real. Deberá incorporar funcionalidades de mensajería instantánea y videollamadas en vivo, que permitan la interacción directa entre el ciudadano o la unidad en campo y el operador CAD para evidenciar en tiempo real la situación reportada desde el sitio de la emergencia en vivo desde su dispositivo móvil sin necesidad de instalar una aplicación, mediante un enlace seguro. Cada transmisión se asocia automáticamente al número de incidente activo y registra coordenadas GPS, hora, operador receptor y metadatos técnicos. Deberá permitir la integración con redes comunitarias y dispositivos de alerta física o digital (botones de pánico, sirenas, sensores ciudadanos), posibilitando la activación inmediata de alertas y el despacho oportuno de recursos siempre que existan los dispositivos, se encuentren en funcionamiento y sean compatibles con los protocolos definidos en la plataforma. Al momento de tipificar el incidente, el módulo despliega automáticamente un conjunto de preguntas predefinidas asociadas al tipo de evento. El contenido de las preguntas es definido y provisto exclusivamente por la Policía Nacional. La calidad, pertinencia y actualización del contenido es responsabilidad exclusiva de la entidad. El administrador carga el contenido mediante la interfaz de configuración del catálogo, sin modificar código fuente. Generación de ID raíz único e irrepetible por incidente (llamada, evento) con prefijo del código DANE (garantiza unicidad nacional entre CADs). Correlación multiagencia dentro del mismo CAD. Mecanismo automático de detección de duplicidades. Historial auditable de todas las modificaciones. Debe permitir la visualización de cámaras cercanas al caso que se encuentre en gestión, por medio de la integración del VMS correspondiente según el tenant en cuestión, dicha visualización debe permitir visualizar cámaras y controlar mediante controles en pantalla. Clasificación de llamadas improcedentes: informativa, molestia, menores, insultos, colgada y equivocada. Se registrará además la calidad de la llamada, el propietario de la línea y la prioridad (rutina, inmediata, flash).		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
	Asociación de una llamada reciente sin caso. La detección de duplicados tendrá radio y ventana de tiempo configurables, y el operador decidirá entre vincular como relacionado o continuar como caso nuevo. Segundo código de tipificación, relato narrativo armado a partir de las respuestas del asistente con notas libres del operador, y cierre rápido sin despacho para casos que no lo requieran. Ubicación asistida: búsqueda de dirección sobre el mapa, coordenadas por clic, geocodificación inversa, casos cercanos y catálogo geográfico de ciudades y barrios. Videollamada: el chat se guardará como evidencia. La grabación se subirá por fragmentos y el sistema cerrará automáticamente las que queden abiertas, registrándolas como adjunto probatorio. Cada caso conservará el historial de sus videollamadas (quién atendió, duración, grabación y chat). Los archivos subidos se validarán por su firma y tamaño. Cámaras: además de un sistema de video central, el sistema soportará un controlador genérico por RTSP, donde el administrador declara los canales. Habrá carga masiva de un censo institucional de cámaras y emparejamiento con las del sistema de video, con revisión manual. El video podrá entregarse en baja latencia mediante una pasarela de medios en un nodo local. El control PTZ ejecutará movimientos acotados con parada garantizada desde el servidor. Se auditará quién vio y quién movió cada cámara. **Admisión de mensajería instantánea.** El canal recibirá mensajes de texto, ubicación, fotografías, audio, video y documentos. • **a)** Un **filtro de ruido** (saludos, cortesías, pruebas) no abrirá caso y responderá una sola vez cómo pedir ayuda. Ante la duda se abre el caso, y todo mensaje que no sea texto (ubicación, foto, audio, video) lo abre siempre. • **b)** Tras abrir el caso, el sistema lo **tipificará de forma guiada** con el catálogo del CAD y solicitará la dirección. El caso queda visible mientras eso ocurre. • **c)** La **ubicación recibida se validará** antes de guardarse (se descartan valores inválidos) y responderá la pregunta de dirección. • **d)** Los **adjuntos** se descargarán al expediente con tamaño máximo y fallos tolerados. Nunca se perderá un caso por no poder traer un adjunto. • **e)** El **operador responderá** desde el caso. El asistente automático se silenciará en cuanto escriba un operador. Se mostrará un **indicador de mensajes sin leer** y el aviso de caso nuevo será inmediato y audible. • **f)** El sistema conectará **proveedores intercambiables** de mensajería, tratados como canal no crítico. **Envío del enlace de videollamada por varios canales.** El orden de intento (mensaje con plantilla aprobada, mensaje de texto libre y SMS) será **configurable por CAD**, con la opción de omitir un canal. Se intentará en orden y gana el primero que funcione. El sistema comprobará antes de intentar mensajería que el destino es un móvil, y dirá al despachador **por qué canal salió** el enlace. Si ninguno funciona, el despachador podrá copiarlo o dictarlo. **Retransmisión de medios propia.** La videollamada usará un servidor de retransmisión propio con **credenciales temporales firmadas**, para funcionar en redes móviles y detrás de cortafuegos, sin depender de servicios de terceros.		
6.9	**Integración ELS / AML:** Ubicación automática del llamante mediante ELS (Google, Android/iOS) y AML (ETSI/EENA). Visualización en capa GIS. Sin requerir app adicional ni datos activos del usuario. La implementación está condicionada a los recursos y acuerdos vigentes entre la Policía Nacional y los operadores móviles del país. Nota: Siempre y cuando		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
	la Policía Nacional tenga acceso, permisos y credenciales a la API de Google que provee el servicio. El sistema consolidará todas las fuentes de ubicación disponibles del caso: localización automática del llamante, ubicación del ciudadano en videollamada, dirección declarada y cámaras cercanas. Mostrará el resultado sobre el mapa como una posición con radio de incertidumbre, que se actualizará y reducirá cuando llegue información más precisa, y registrará la fuente de cada dato. La geocodificación soportará la nomenclatura urbana colombiana (calles, carreras, diagonales, transversales, esquinas y barrios), y el operador validará la dirección cuando la confianza sea baja. La ubicación del llamante se consultará a través de un proveedor configurable de forma centralizada, con credenciales cifradas y nunca visibles en pantalla. Cada posición registrará su origen y la hora en que fue tomada, y la consulta tendrá un tiempo máximo de espera, tras el cual el operador continuará sin ella.		
6.10	**Módulo de Analítica e IA Asistida:** Transcripción automática de voz a texto de las grabaciones de llamadas recibidas desde la planta telefónica institucional. La transcripción opera de forma asíncrona sobre el archivo de audio una vez finalizada la llamada (no en tiempo real durante la llamada), generando un texto asociado al registro del incidente. Sobre la transcripción se aplica extracción automática de: dirección, barrio, punto de referencia, tipo de emergencia, número de heridos y placas vehiculares. La información extraída se presenta al operador como sugerida para el formulario — el operador valida y decide qué usar. Ningún campo se autocompleta sin intervención del operador. Este módulo puede ser habilitado o deshabilitado por el administrador sin afectar la operación del sistema. La transcripción está condicionada a que la planta telefónica provea archivos de audio en formato compatible (formatos definidos en mesas de trabajo iniciales). Integración con dashboards de OFTIC. En caso tal de que no se pueda integrar el audio de la planta, validar la posibilidad de integrar el agente de transcripción en tiempo real, siempre que las latencias sean adecuadas para una plataforma de misión crítica y que sea viable en los plazos y alcances del proyecto. Además de la transcripción asíncrona, el módulo podrá ofrecer **transcripción en vivo** durante la llamada, con extracción sugerida de dirección, punto de referencia, tipo de emergencia, heridos y placas, y un **resumen automático** al cierre. La latencia aceptable se definirá en mesas de trabajo [a definir]. Todo el procesamiento se hará en la infraestructura de la entidad, sin enviar audio ni texto a servicios externos. El contratista especificará los requisitos de hardware para la concurrencia solicitada [a definir]. Toda recomendación del motor indicará **en qué datos se basa** y quedará registrada en auditoría, junto con la decisión del operador. El operador valida y decide siempre. El sistema **no** autocompletará campos ni despachará recursos de forma automática, y no realizará análisis de emociones ni perfilamiento de personas. **Resúmenes automáticos.** A partir de la transcripción, las anotaciones y los datos del caso, el sistema generará un resumen breve en los siguientes momentos: (i) al cierre de la llamada, (ii) al cambiar de turno, para el relevo, y (iii) al remitir el caso a una agencia o a otro CAD. Un usuario autorizado podrá pedir el resumen de cualquier caso que ya pueda ver, y recibirá un texto de extensión máxima [a definir]. El resumen **se presentará como sugerencia editable**		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
	y indicará de qué datos proviene. Quedará registrado quién lo aprobó antes de enviarse a un tercero.		
6.11	**Gestión de incidentes:** Funcionalidad que permite la gestión integral del caso desde su creación hasta el cierre, enlazando los datos provenientes de la recepción multicanal con los procesos de clasificación, asignación, seguimiento y finalización. Registra automáticamente (cuando sea técnicamente viable) la información del ciudadano, tipo de incidente, ubicación, recursos desplegados y entidades involucradas. Cada evento se vincula con el número único de incidente y mantiene trazabilidad completa de las acciones, comunicaciones, tiempos de respuesta y decisiones operativas. Debe disponer de dos vistas, una donde se evidencian los incidentes remitidos por el operador, con semaforización configurable por tiempos, tipo de incidente o importancia e información relevante. La otra vista se abre cuando el operador oprime sobre el incidente en la lista, esta debe permitir gestionar todo lo relacionado al caso, asignar recursos, añadir comentarios, despachar a otras agencias remotas, tipificar o clasificar el incidente, entre otras funcionalidades las cuales se darán a conocer en mesas de trabajo iniciales. Integra mapa para la localizar medios o recursos disponibles cercanos al lugar del incidente. Debe permitir registrar actividades operativas y preventivas asociadas al incidente, así como novedades de personal. Bandeja por canal de atención con contadores por estado, refresco automático y alerta sonora de casos nuevos. El mapa del caso mostrará los recursos en movimiento y la ubicación del ciudadano. Todo cambio manual de estado exigirá un motivo y quedará en un historial. La reapertura de un caso cerrado requerirá autorización. Control de atención: registro del primer acceso, alertas por casos sin abrir y por gestión prolongada (umbrales parametrizables) y presencia concurrente. Actuaciones por unidad con su ciclo (asignado, despacho, en sitio, cierre), varias unidades por actuación, notas, desasignación, resultado, clasificación operativa o preventiva y catálogos de actividades y delitos. El cierre admitirá múltiples códigos y exigirá confirmación. Solicitud y atención de apoyo urgente por seguridad del funcionario. Remisión del caso a otros canales o agencias, con opción de conservarlo o transferirlo, y visibilidad multicanal. Plantillas de anotación, anotación del supervisor inmutable y tablero de indicadores por operador. Recomendación de recursos por **tiempo estimado de llegada**, calculado sobre la red vial y no solo por distancia. Considerará estado y capacidad de la unidad, y mostrará al operador las alternativas con su tiempo. **Posicionamiento dinámico:** a partir del histórico de demanda por zona y franja horaria, el sistema sugerirá dónde ubicar las unidades disponibles para reducir el tiempo de respuesta. Será una sugerencia, no una orden.		
6.12	**GIS Interno 2D:** Módulo GIS con mapas 2D, rutas dinámicas y geocercas. Capas de contexto: priorización de incidentes, niveles Ciudad/Región/Departamento/Nación, capa policía, entidades médicas, bomberos, ejército, otras agencias, cámaras integradas vía VMS. Capas		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
	históricas: mapas de calor, histórico por eventos, zonas con más eventos, indicadores (mínimo 3), reportes. Integración con cartografía y licencias ARCGIS de la Policía Nacional cuando aplique. Imagen operativa común del territorio del CAD. Capas de contexto: priorización de incidentes, niveles Ciudad/Región/Departamento/Nación, capa policía/médica/bomberos/ejército/otras agencias, recursos compartidos, cámaras integradas vía VMS. Capas históricas: mapas de calor, histórico por agencia/eventos, zonas con más eventos, históricos operacionales, indicadores, reportes. Herramienta de reproducción cronológica post-evento. La Policía Nacional proveerá acceso a licencias ARCGIS institucionales cuando aplique. Mapa de incidentes en vivo con filtros por canal y colores por prioridad. Mapa estadístico con filtros por ciudad, barrio, turno y fechas.		
6.14	**Anotaciones Generales:** Permite registrar anotaciones generales durante el turno, tales como: comunicados, revistas, actividades operativas o preventivas, novedades con personal y cualquier información que durante la actividad de policía deba registrarse. Debe generar un ID único por registro.		
6.15	**Reportes:** Permite generar informes estadísticos, visualizar y descargar reportes que permitan evaluar la actividad de los usuarios del sistema y de los recursos en campo respecto a la atención de incidentes (Tiempos de atención, medios utilizados). Asimismo, deberá generar reportes que permitan identificar el comportamiento del ingreso de llamadas, creación y gestión de incidentes. Deberá permitir visualizar el ciclo de vida de un incidente, mostrando el flujo desde su creación hasta el cierre, identificando responsables e intervinientes. Informes de calidad, efectividad, tiempos, operadores y códigos, con exportación a CSV, panel de SLA, filtro por turno e informe imprimible del análisis estadístico. **Consulta en lenguaje natural.** El usuario podrá escribir una consulta en lenguaje corriente (por ejemplo, tipo de incidente, zona, periodo y franja horaria) y el sistema la traducirá a los filtros de los reportes existentes. El sistema **mostrará siempre los filtros que aplicó**, para que el analista los verifique y los ajuste. La consulta se limitará a **operaciones de lectura** sobre los datos que el usuario ya tiene permiso de ver, y cada consulta quedará en auditoría con el texto escrito y los filtros resultantes. Si no puede interpretarla, lo dirá y no inventará un resultado.		
6.16	Asistente Inteligente de Atención: Guía de preguntas orientadoras activada automáticamente al tipificar el incidente. El contenido de las preguntas, su asociación a tipos de incidente y el orden de presentación serán definidos y provistos por la Policía Nacional antes del inicio de la implementación. El administrador del sistema cargará el contenido vía interfaz de configuración, sin modificar código fuente. Administración del catálogo de tipificación (alta, edición, estado, importación masiva con plantilla y vínculo a la categoría del asistente). Las preguntas del asistente admitirán distintos tipos de respuesta, obligatoriedad, ayuda y orden.		
6.17	**Auditoría y Logs:** Registro digital automático de todas las llamadas y acciones del sistema. Trazabilidad operativa completa de sesiones, actividades y cambios. Una vez entregado exitosamente un caso a una agencia externa (confirmado por log), la trazabilidad dentro de los sistemas de terceros es responsabilidad de cada agencia		
6.18	**Continuidad DRP:** Alta disponibilidad 24/7. Valoración de riesgo (impacto/probabilidad). Definición de sitios alternos. Diseño, implementación y pruebas de DRP. Simulacros periódicos con registro de lecciones aprendidas		
6.19	**Sincronización de Tiempo:** Sincronización horaria precisa mediante NTP (Network Time Protocol es el estándar utilizado para sincronizar los relojes de los sistemas informáticos a		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
	través de una red. Garantiza que todos los componentes "hablen" en el mismo instante temporal.). Servidor maestro y secundario con conmutación automática en máximo 30 segundos. Timestamps en UTC con visualización en UTC-5 (Colombia). Precisión máxima ±1 segundo respecto al servidor de referencia. Ante pérdida de conectividad NTP, cada nodo mantiene su última referencia y registra el período de desincronización en auditoría.		
6.20	**Manejo de Colas ACD:** Distribución automática omnicanal (voz, chat, SMS). Skills-based routing. Estados de agente configurables. Monitoreo en tiempo real: volumen, ASA, abandonos, SLA. ID de grabación con trazabilidad al incidente obtenido de la integración la planta telefónica. Integración CTI/SIP. El sistema debe integrarse con la planta telefónica con el fin de evidenciar el numero abonado que origina la llamada de emergencia. Asimismo, debe integrarse con el aplicativo Webex encargado de establecer comunicaion entre el operador y el ciudadano. El operador atenderá y realizará llamadas desde un **teléfono integrado en el navegador** (señalización SIP y audio por WebRTC), sin instalar software ni equipo adicional. La cola repartirá las llamadas entre los operadores **conectados y disponibles**. Cuando nadie conteste en el tiempo configurado, la llamada **se desbordará** al destino definido por el CAD, y el sistema registrará que fue desbordada. Al contestar, el sistema **abrirá el caso** con los datos de la llamada (número de abonado y los datos disponibles). El operador podrá **llamar desde el caso**, y el sistema ordenará primero la llamada al operador y después al ciudadano. Cada grabación quedará **asociada al incidente** y bajo custodia del caso, con su identificador de grabación. Las llamadas salientes también se grabarán. La central y sus parámetros (troncales, números, desborde, credenciales de los operadores) se **administrarán desde la aplicación**, sin intervención manual sobre el servidor. La configuración se generará desde el sistema. El sistema aceptará **distintos proveedores de planta** mediante una interfaz común, de modo que cambiar de proveedor no obligue a modificar el resto de la aplicación. Cuando la planta institucional no provea ACD, el sistema podrá operar con una **central propia por CAD**, con una planta por CAD sobre infraestructura compartida y supervisión de su estado.		
6.21	**Interoperabilidad:** Exposición controlada de información: datos abiertos e históricos accesibles vía API. API Manager para integración con entidades y demás instituciones públicas o privadas, hasta N integraciones por CAD. Tableros y reportes de cara al ciudadano o agencias. Soporte tecnológico a la planta telefónica y al sistema de gestión de llamadas de emergencia y no emergencia. Cumplimiento de estándares NG911/NG112/NENA i3. Todos los servicios de la plataforma sincronizan su referencia temporal mediante NTP con desviación máxima ±1 segundo. Servidor NTP maestro con secundario de respaldo y conmutación automática en ≤30 segundos. Timestamps en UTC con conversión a UTC-5 para interfaces. La conectividad estable a los servidores NTP de referencia (ej. ntp1.inm.gov.co) es responsabilidad de la Policía Nacional.		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
	El sistema debe disponer de una interfaz “Hub de Integraciones” la cual permita gestionar todas las integraciones de la plataforma, integraciones salientes, entrantes, planta telefónica, proveedor SMS, proveedor de cámaras VMS y auditoria, por tenant. El sistema implementará, de forma progresiva y según los acuerdos con los operadores de telefonía, los estándares abiertos de intercambio de datos de emergencia (NG112/NENA i3 y los asociados), con un plan de adopción por etapas.		
6.22	**Personalización institucional.** Nombre, sigla, logo e ícono del sistema, imágenes rotativas de acceso, video institucional, noticias, comunicados y ventanas informativas.		
6.23	**Accesibilidad.** Cumplimiento de WCAG 2.1 nivel AA: texto escalable en siete niveles, modo oscuro, lectura en voz alta y dictado por voz.		
6.24	**Cadena de custodia de la evidencia.** Las grabaciones de llamadas y videollamadas, los chats y los adjuntos se sellarán con huella criptográfica y hora, y se registrará cada consulta, descarga o exportación (quién, cuándo y desde dónde). El sistema permitirá verificar que un archivo no fue alterado y generar un informe de custodia por caso.		
6.25	Capacitación, simulación y calidad. • a) Entorno de simulación con incidentes sintéticos, aislado de la operación real, para entrenar y evaluar operadores. • b) Control de calidad de la atención: cumplimiento del protocolo de preguntas, tiempos de cada etapa y preguntas omitidas, con muestreo y revisión por un supervisor, y retroalimentación al operador. • c) Reproducción cronológica de un incidente (llamada, mapa, acciones y recursos) para análisis posterior.		
6.26	**Analítica predictiva.** Proyección de demanda por zona, franja y tipo de incidente, y recomendación de dotación de **operadores y unidades** por turno. Los modelos se entrenarán con el histórico del propio CAD y los datos personales permanecerán en el CAD territorial. El sistema comparará en tiempo real el ingreso de llamadas y casos por zona y franja con el comportamiento histórico de ese mismo CAD. Cuando detecte un aumento atípico, **alertará al supervisor** indicando la zona, el tipo de incidente y la magnitud, y **no actuará por sí mismo**. Los umbrales de sensibilidad serán configurables por CAD y se medirá la tasa de falsas alertas [a definir en mesas de trabajo].		
6.27	**Transferencia entre CAD.** Cuando un hecho corresponda a la jurisdicción de otro CAD, el sistema permitirá transferir el caso con todo su contexto (datos, ubicación, anotaciones, adjuntos y videollamada), con trazabilidad en ambos CAD y confirmación de recepción.		
6.28	**Indicadores de desempeño.** El sistema medirá y mostrará, por CAD y por turno, como mínimo: tiempo desde el ingreso de la llamada hasta el despacho, tiempo hasta obtener una ubicación confiable, tiempo de llegada de la unidad, porcentaje de casos despachados con la primera recomendación y cumplimiento del protocolo de atención. Las metas se fijarán en las mesas de trabajo [a definir].		
6.29	**Tablero de sala y monitoreo en vivo.** El sistema ofrecerá una pantalla de sala de operaciones, apta para proyectarse, con la cola de llamadas, los casos activos por estado, el estado de la central y la salud del CAD, actualizada en tiempo real y sin interacción. Producirá un informe en PDF de las métricas de atención por periodo. Medirá el consumo por CAD (llamadas, mensajes y almacenamiento).		
7	**ARQUITECTURA Y TECNOLOGÍA DE SOFTWARE - REQUISITOS NO FUNCIONALES**	**CUMPLE**	**NO CUMPLE**
7.1	**Arquitectura:** Microservicios contenerizados (Docker/Kubernetes). Servicios globales: Auth, Tenant Resolver, Connection Pool Manager, API Gateway, Analytics ETL. Servicios por tenant: CAD Core, Dispatch Engine, GIS, Communication Hub, AI Service. Servicios edge: microservicios mínimos de despacho en nodos locales**.** Al inicio del proyecto se definira en mutuo acuerdo los servicios a implementar en la arquitectura.		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
7.2	**Multitenant DB-per-Tenant:** Aislamiento completo de datos operativos entre CADs. Schema idéntico para todos los tenants gestionado con Flyway/Liquibase Licenciamiento Open Source. Enrutamiento mediante Connection Pool Manager con credenciales cifradas en Vault.		
7.3	**Código Abierto:** Desarrollada con lenguajes y tecnologías de código abierto sin dependencias propietarias para funciones críticas. Lenguajes principales: Java o Python o C# .NetCore (últimas versiones estables).		
7.4	**Sistema Operativo Servidores:** Distribución Linux (preferida). En caso de requerirse, Windows Server Standard con licencia Open Value registrada a nombre de la Policía Nacional, con soporte mínimo 3 años. El contratista especificará en su oferta el sistema operativo de cada grupo de servidores.		
7.5	**Escalabilidad:** Horizontal: nuevos servidores físicos sin interrupción. Vertical: independiente por tenant. SLA ≥99.95% servicios globales. SLA ≥99.9% por tenant.		
7.6	**Usabilidad:** Interfaces UX/UI accesibles desde navegadores estándar (Firefox, Chrome, Safari). Compatibilidad con Android, iOS y escritorio. PWA para carga offline de la interfaz. El contratista especificará versiones compatibles de cada navegador. El sistema estará disponible únicamente en red de Policía Nacional (Polired)		
7.7	**Ambientes:** Mínimo 3 ambientes con soporte multitenant: Desarrollo, Pruebas (construcción) y Producción (con backup de data estructurada y no estructurada). Las grabaciones antiguas se moverán de la base de datos a almacenamiento de objetos sin borrarse, con proceso programado, límite por pasada y bloqueo para que dos instancias no archiven lo mismo. Los parámetros de antigüedad serán configurables [a definir]. La bitácora tendrá una política de retención configurable. El respaldo se verificará restaurándolo en una base temporal, y el resultado quedará registrado. Las copias de seguridad no se almacenarán junto con la clave que cifra los secretos.		
7.8	**Procesamiento**: Arquitectura de procesamiento paralelo y distribuido para tareas simultáneas en múltiples servidores. Orquestación de contenedores para portabilidad, escalabilidad y resiliencia operativa.		
7.9	**Protección de Datos:** Cumplimiento Ley 1581 de 2012. Datos personales de ciudadanos permanecen en BD del CAD territorial. El Data Warehouse de analítica solo recibe datos pseudoanonimizados.		
8	**LICENCIAMIENTO - CESIÓN DE DERECHOS PATRIMONIALES**	**CUMPLE**	**NO CUMPLE**
8.1	El contratista deberá transferir a título gratuito todos los Derechos Patrimoniales del objeto del contrato a través del documento anexo “CONTRATO DE CESIÓN DE DERECHOS PATRIMONIALES DE AUTOR” y debe estar debidamente registrado ante la Dirección Nacional de Derechos de Autor Unidad Administrativa Especial del Ministerio del Interior y protocolizado ante notaría. El contratista debe registrar el presente contrato en la entidad competente para el Registro de Derecho de Autor y remitir el certificado de inscripción como requisito previo para la suscripción del acta de recibo final a satisfacción y para la realización del último contador de pago correspondiente para cada uno de los desarrollos implementados.		
8.2	Los trámites de firmas de notaría por registro de firma y huella de la cesión de derechos patrimoniales no deberán generar costo para la Policía Nacional.		
8.3	El contratista debe anexar como documentos entregables al contrato el CONTRATO DE CESIÓN DE DERECHOS PATRIMONIALES DE AUTOR y copia del CONTRATO DE CESIÓN que se realizó entre los empleados contratados y la firma contratante, donde transfieren los derechos a la empresa.		
8.4	En caso de ser necesario el licenciamiento, este deberá ser válido a nivel nacional, ya que el acceso al sistema de información se realizará desde todas las regionales y centros zonales del país.		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
8.5	Dada la diversidad de las aplicaciones que se implementarán, en caso de que alguna de ellas requiera la incorporación de software base adicional para su construcción o mantenimiento, las licencias correspondientes deberán ser entregadas a la Policía Nacional, y serán de su propiedad a perpetuidad. Asimismo, el licenciamiento de uso de las aplicaciones será propiedad de la Policía Nacional.		
8.6	El contratista deberá entregar la totalidad del código fuente correspondiente al software, en formato magnético editable, junto con los manuales elaborados (editables), también en formato magnético, una vez finalizada la etapa de implementación. Los entregables deben estar debidamente rotulados y respaldados con la documentación que describa su contenido.		
8.7	Cada uno de los componentes de software necesarios para llevar a cabo el presente proceso deberá ser licenciado y entregado a nombre de la Policía Nacional.		
8.8	Con la oferta, el contratista deberá enunciar cada uno de los softwares a utilizar, especificando qué labor o función de las solicitadas será soportada por cada uno de ellos. Todos los plugins, complementos y funcionalidades adicionales necesarias para el correcto funcionamiento del sistema deberán ser incluidos en la oferta.		
8.9	En caso de que la oferta no incluya el software necesario para cumplir con el objeto del presente proceso, la oferta será considerada técnicamente no válida.		
8.10	En los casos en que el licenciamiento sea por uso, cantidad de segundos, palabras, bits o cualquier otra modalidad definida por el fabricante, el contratista deberá garantizar su uso sin costos adicionales para la Policía Nacional durante los períodos de soporte y garantía establecidos en el presente estudio previo. Además, deberá entregar junto con el recibo de satisfacción las condiciones de uso aplicables durante dichos períodos de garantía y soporte		
8.11	El licenciamiento del software debe cubrir todas las implementaciones e integraciones necesarias con los sistemas de la Policía Nacional requeridas para el presente proyecto		
8.12	El contratista deberá realizar el despliegue del compilado del proyecto en el entorno utilizado y administrado por la Policía Nacional. El despliegue debe garantizar la compatibilidad y el correcto funcionamiento del proyecto dentro del ecosistema gestionado por la Policía Nacional, cumpliendo con las políticas de seguridad y administración establecidas.		
8.13	Entrega del Proyecto en Repositorio de DevOps El contratista deberá entregar el proyecto completo en el repositorio de DevOps administrado por la Oficina de Tecnologías de la Información y de las Comunicaciones (OFTIC). Dicha entrega deberá cumplir con las siguientes condiciones: **1. Rama Master:** el código fuente deberá estar actualizado y consolidado en la rama principal (master), asegurando que esta contenga la versión final funcional y aprobada del proyecto. **2. Historial de cambios:** el repositorio deberá incluir el historial completo de cambios realizados durante el desarrollo, garantizando la trazabilidad de las modificaciones. **3. Estructura estándar:** la estructura del repositorio deberá estar organizada de manera que facilite la comprensión, mantenimiento del código, siguiendo las prácticas recomendadas de DevOps. **4. Accesos y credenciales:** el contratista deberá coordinar con la OFTIC para obtener los accesos necesarios al repositorio de DevOps. En ningún caso se permitirá el uso de repositorios externos o plataformas no gestionadas por la institución. **5. Validación final:** la entrega del proyecto en el repositorio será validada por el equipo técnico de la OFTIC, quien verificará que se cumplan todos los lineamientos y requisitos establecidos.		
9	**SOPORTE, MANTENIMIENTO Y GARANTÍA**	**CUMPLE**	**NO CUMPLE**
9.1	**Mantenimiento:** Plan de mantenimiento preventivo y correctivo. Actualizaciones de firmware anuales (o cuando el fabricante libere versión estable). Plan de replicación en sitio alterno para continuidad operacional. **Mesa de ayuda integrada.** Desde la aplicación el usuario podrá abrir un ticket que incluirá un informe de diagnóstico automático (versión publicada, errores recientes, canal y entorno). Cada ticket se clasificará con una matriz de severidad documentada, con tiempos de atención por nivel [a definir].		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
9.2	**Soporte software:** 24x7 desde recibo a satisfacción. Mesa de servicio web, línea telefónica y correo electrónico. Incidencias alto impacto: atención inicial ≤2 horas. Solución definitiva ≤48 horas. Garantía software: 1 año. El contratista deberá disponer del personal necesario para brindar soporte a los usuarios del sistema a través de servicio telefónico, presencial y por correo electrónico. Además, deberá capacitar a un grupo de usuarios de la Policía Nacional, quienes también estarán capacitados para brindar soporte.		
9.3	Se deberá contemplar la detección y corrección de las fallas de la solución implementada, así como el suministro y/o reemplazo de los módulos de aplicación que presenten daños o deficiencias en su funcionamiento.		
9.4	Las actualizaciones de versión o mejoras como por ejemplo en el GUI (interfaz gráfica) que se requieren para su normal funcionamiento que hagan parte del levantamiento de requerimientos inicial del proyecto deben ser asumidas por el contratista, durante el periodo de garantía.		
9.5	El contratista se compromete a subsanar los fallos y defectos que se presenten en el software implementado, así como cualquier inconveniente en sus funcionalidades, durante el período de garantía solicitado, contado a partir de la fecha de entrega a satisfacción. En caso de que los fallos o defectos no puedan ser subsanados, el contratista deberá proporcionar una solución alternativa que permita la continuidad de la operación de la plataforma. Además, el contratista asumirá los costos de los recursos humanos o tecnológicos necesarios para implementar dicha solución alternativa		
9.6	**Acompañamiento:** Mínimo 3 meses desde entrega a satisfacción para estabilización, ajustes de configuración y recomendaciones de mejora.		
10	**SEGURIDAD, CUMPLIMIENTO Y POLÍTICAS**	**CUMPLE**	**NO CUMPLE**
10.1	**Seguridad de información:** Personal del proyecto sujeto a estudio de seguridad llevado a cabo por la Dirección de Inteligencia de la Policía Nacional durante la vigencia del contrato. Firma de acuerdo de confidencialidad (Formato 1DT-FR-0010 o vigente según Res. 04408/2024). Cumplimiento del SGSI (Resolución 08310 del 28/12/2016). En caso de que alguno de los colaboradores involucrados no apruebe dicho estudio, el contratista estará obligado a reemplazar a la persona en cuestión por otra que cumpla con las mismas condiciones de experiencia exigidas, quien también deberá someterse al estudio de seguridad. En virtud del presente contrato, el contratista se compromete a no divulgar ninguna información que obtenga o conozca durante la ejecución del mismo que esté marcada como confidencial. Esto incluye, pero no se limita, a la información relacionada con los lugares a los cuales tenga acceso con motivo de su desarrollo, así como cualquier otra información considerada confidencial. El contratista deberá firmar el formulario de acuerdo de confidencialidad correspondiente.		
10.2	**Seguridad multitenant:** Aislamiento de red por tenant (VLAN/VPC). Validación de tenant en cada request. JWT con claims de tenant. Cross-tenant access denegado y auditado. Pruebas de penetración cross-tenant. OWASP Top 10 + guías multitenant.		
10.3	**Seguridad IA:** Procesamiento 100% local. Bloqueo de egress para inferencia. Auditoría de consultas al motor de IA**.**		
10.4	**Política ambiental**: Cumplimiento de la Política Ambiental de la Policía Nacional. Disposición final de RAEE según Ley 1672/2013.		
10.5	**SST:** Cumplimiento Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST). EPP durante instalación, ARL vigente. El contratista deberá cumplir con la implementación del sistema de Gestión de la Seguridad y Salud en el Trabajo, para lo cual deberán diligenciar el Formulario Sistema de Gestión de la Seguridad y Salud en el Trabajo.		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
10.6	**Anticorrupción:** Compromiso anticorrupción. Incumplimiento = causal de rechazo de oferta o terminación anticipada del contrato. El contratista se compromete a cumplir con las políticas de anticorrupción dentro del proceso, manifestando su disposición a suministrar toda la información necesaria para asegurar la transparencia del mismo. En caso de comprobarse el incumplimiento de este compromiso por parte del contratista, sus empleados, representantes, asesores o cualquier otra persona que actúe en su nombre durante el proceso de contratación, dicho incumplimiento será motivo suficiente para el rechazo de la oferta o la terminación anticipada del contrato, si dicho incumplimiento ocurre después de la adjudicación. Para este efecto, el contratista deberá diligenciar el formulario de compromiso anticorrupción.		
11	**CAPACITACIÓN**	**CUMPLE**	**NO CUMPLE**
11.1	El contratista deberá realizar una transferencia de conocimiento de al menos 40 horas en las instalaciones que la Policía Nacional indique, dirigida a un mínimo de 8 personas, en temas de desarrollo de software relacionados al proyecto que el supervisor indique.		
11.2	El contratista realizará capacitación técnica al personal de la Policía Nacional designado por el Supervisor del Contrato, sobre el código fuente de la solución implementada, en cada etapa del proyecto, hasta su puesta en producción.		
11.3	Capacitación operativa territorial: El contratista deberá ejecutar una estrategia de transferencia de conocimiento bajo el esquema de “Formación de Formadores”, mediante la capacitación centralizada de personal designado por la entidad, quienes actuarán como multiplicadores de conocimiento a nivel territorial. La capacitación deberá contemplar componentes teóricos y prácticos orientados a perfiles operativos, técnicos, funcionales y administrativos del sistema. Como parte de sus obligaciones, el contratista deberá suministrar el material didáctico, manuales, guías operativas, presentaciones y laboratorio para garantizar la réplica interna del conocimiento por parte de la entidad en los diferentes territorios donde se implemente la solución.		
11.4	**Capacitación especializada en desarrollo:** El contratista deberá realizar una transferencia de conocimiento de al menos 40 horas en las instalaciones de la Dirección General de la Policía Nacional o en cualquier otra oficina que la entidad indique en la ciudad de Bogotá, dirigida a un mínimo de 8 personas designadas por el supervisor, esta transferencia de conocimiento estará enfocada en temas de arquitectura de software y el código fuente de la solución implementada. **1. Arquitectura del Sistema CAD:** • Diseño, componentes y flujos internos. • Arquitectura basada en microservicios, enrutamiento, balanceo de carga y alta disponibilidad. • Interoperabilidad mediante APIs, colas de mensajes, integración multiagencia. **2. Desarrollo y Mantenimiento de Software:** • Estructura del código fuente entregado. • Guías de extensión y mantenimiento evolutivo. • Estándares de codificación en JavaScript y Python utilizados en el proyecto. • Metodologías ágiles (Scrum/Kanban) aplicadas al sistema. **3. Bases de Datos e Integración:** • Administración del motor de base de datos en uso (Oracle, PostgreSQL u otros definidos en el proyecto). • Replicación, respaldos, restauración y monitoreo.		

	DESCRIPCIÓN DEL REQUERIMIENTO	CUMPLE	NO CUMPLE
	• Diseño de esquemas para incidentes, despachos y trazabilidad. **5. Infraestructura y DevOps:** • Pipeline de despliegue, automatización, pruebas y monitoreo. • Contenedores, imágenes Docker, seguridad y operación. • Gestión de logs, telemetría, análisis de desempeño y escalabilidad.		